

UNITED STATES PATENT APPLICATION

for

**DISCOURAGING UNAUTHORIZED REDISTRIBUTION OF PROTECTED
CONTENT BY CRYPTOGRAPHICALLY BINDING THE CONTENT TO INDIVIDUAL
AUTHORIZED RECIPIENTS**

Applicants:

Michael S. Ripley
Jeffrey B. Lotspiech

prepared by:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Boulevard
Los Angeles, CA 90026-1026
(303) 740-1980

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL807366952US

Date of Deposit June 27, 2001

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Debbie Peloquin

(Typed or printed name of person mailing paper or fee)

Debbie Peloquin

(Signature of person mailing paper or fee)

**DISCOURAGING UNAUTHORIZED REDISTRIBUTION OF PROTECTED CONTENT BY
CRYPTOGRAPHICALLY BINDING THE CONTENT TO INDIVIDUAL AUTHORIZED RECIPIENTS**

COPYRIGHT NOTICE

[0001] A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

FIELD OF THE INVENTION

[0002] This invention relates to static and dynamic information storage and retrieval. More particularly, this invention relates to methods, apparatus and systems for the protection of stored information from unauthorized copying.

BACKGROUND OF THE INVENTION

[0003] Accompanying the widespread conversion of many types of content, such as movies, music, books, etc., to digital formats has been the development of a number of systems for protecting such content against unauthorized access, reproduction, and distribution. In many such protection systems, the content is encrypted such that access requires a decryption key, which is made available under terms agreeable to the content owner/provider.

[0004] To prevent unauthorized reproduction and redistribution of such protected content, the encryption key is often also made dependent on some unique or relatively unique identifier associated with the original storage medium or device to which the content is bound. This dependency can be implemented using, for example, a cryptographic function of the identifier. If the content is copied to another storage medium or device, the decryption key formed using the identifier of that other medium or device will be different from the original encryption key, thereby preventing access to the unauthorized copy.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0006] FIG. 1 is a diagram illustrating concepts and functionality within embodiments of the invention.

[0007] FIG. 2 is a high level flow chart illustrating a method to bind content to a customer identifier in accordance with embodiments of the invention.

[0008] FIG. 3 is a high level flow chart illustrating a method to access content that is bound to a customer identifier in accordance with exemplary embodiments of the invention.

[0009] FIG. 4 is a detailed flow chart illustrating a method to bind content to a customer identifier in accordance with embodiments of the invention.

[0010] FIG. 5 is a detailed flow chart illustrating a method to access content that is bound to a customer identifier in accordance with exemplary embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0011] In one aspect of the invention, a method is disclosed for providing a means of discouraging unauthorized reproduction and redistribution of protected content by binding content to an individual to whom the content is originally provided. It may be used in conjunction with one or more other protection schemes, such as a protection scheme that binds the content to the storage medium, or it may be used in lieu of other protection schemes.

[0012] In an exemplary embodiment, an on-line service (hereinafter "service") sells digital content, such as music titles, to its customers (hereinafter "customers"). In this embodiment, a customer selects a title, and the service binds the title to an identifier associated with the customer (hereinafter "Customer I.D."). The title can then be downloaded to the customer. As a result, the Customer I.D. is needed in order to access the content. If the content is redistributed, it is useless to anyone that receives it unless the receiver also receives the Customer I.D. to which the content is bound.

[0013] The present invention includes various operations, which will be described below. The operations of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations. Alternatively, the operations may be performed by a combination of hardware and software.

[0014] The present invention may be provided as a computer program product which may include a machine-readable medium having stored thereon instructions which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs (Compact Disc-Read Only Memories), and magneto-optical disks,

ROMs (Read Only Memories), RAMs (Random Access Memories), EPROMs (Erasable Programmable Read Only Memories), EEPROMs (Electromagnetic Erasable Programmable Read Only Memories), magnetic or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions.

[0015] Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer (e.g., a server) to a requesting computer (e.g., a client) by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection). Accordingly, herein, a carrier wave shall be regarded as comprising a machine-readable medium.

Introduction

[0016] In embodiments of the invention, concepts used herein are derived from current schemes for content protection, including Content Protection For Recordable Media (CPRM).

[0017] Generally, a device for using content, such as for playback or recording, (hereinafter "device", such as a hardware DVD player/recorder, or a software player/recorder used in conjunction with a computer equipped with a DVD drive) is given a set of n Device Keys denoted K_{d_0} , K_{d_1} , ..., K_{d_n-1} . These keys are provided by the 4C Entity, LLC, and are for use in processing the MKB (Media Key Block) to calculate the Media Key (K_m). Key sets may either be unique per device, or used commonly by multiple devices.

[0018] For each Device Key there is an associated Column and Row value, referred to as Cd_i and Rd_i ($i=0,1,\dots,n-1$) respectively. Column and Row values start at 0. For a given device, no two Device Keys will have the same associated Column value (in other words, a device will have at most one Device Key per Column). It is possible for a device to have some Device Keys with the

same associated Row values. The number of Device Keys that are given to each device and the range of Column and Rows values that are possible may be defined separately for each device type. A device treats its Device Keys as highly confidential, and their associated Row values as confidential.

[0019] In the case of content protected by CPRM, for example, on a DVD (Digital Versatile Disc), media manufacturers place the following on each piece of CPRM compliant media:

[0020] • A prerecorded Media Identifier (ID_{media}).

[0021] • A prerecorded Media Key Block (MKB).

[0022] CPRM recorders then record the following onto a writable area of the compliant media:

[0023] An encrypted title key.

[0024] An encrypted title (i.e. content encrypted using the title key).

Media Identifier

[0025] A Media Identifier comprises a value on which access to protected content depends. Typically, the value is unique for every medium.

Media Key Block

[0026] The Media Key Block (MKB) is generated by the 4C Entity, LLC, and allows all compliant devices, each using their set of secret Device Keys, to calculate the same Media Key (K_m). If a set of Device Keys is compromised in a way that threatens the integrity of the system, an updated MKB can be released that causes a device with the compromised set of Device Keys to calculate a different K_m than is computed by the remaining compliant devices. In this way, the compromised Device Keys are "revoked" by the new MKB.

[0027] An MKB is formatted as a sequence of contiguous records, where each record begins with a record type field, followed by a record length field. An MKB is part of an MKB Frame that is constructed from n MKB Packs having data. Each MKB Frame begins with an MKB Descriptor, which is part of the first MKB Pack, or MKB Pack #0. Each of the first n-1 MKB Packs are filled completely. The nth MKB Pack may end up with unused bytes, which are zero-filled.

[0028] In order to process the MKB, each authorized device receives a set of “n” Device Keys. Using its Device Keys, a device calculates the Media Key by processing records of the MKB one-by-one from first to last. After processing of the MKB is completed, the device uses the most recently calculated Media Key value as the final value for the Media Key.

[0029] If a device correctly processes an MKB using Device Keys that are revoked by that MKB, the resulting final Media Key will have the special value 0H, where H designates a hexadecimal number. This special value will never be an MKB’s correct final Media Key value, and can therefore always be taken as an indication that the device’s keys are revoked. If a device calculates this special Media Key value, it stops the authentication, playback, or recording session in progress, and will not use that Media Key value in any subsequent calculations.

[0030] A properly formatted MKB will have exactly one Verify Media Key Record (VMKR) as its first record. The VMKR contains the hexadecimal value DEADBEEF encrypted with the correct, final Media Key. The presence of the VMKR is mandatory, but the use of the VMKR by a device is not mandatory. A device may attempt to decrypt the VMKR using its current Media Key value during the processing of subsequent Records, checking each time for the hexadecimal value DEADBEEF. If the device successfully decrypts the VMKR, the device has already calculated the correct final Media Key value, and may therefore stop processing the MKB.

[0031] A properly formatted MKB will have exactly one calculate Media

Key record (CMKR). Devices must ignore any CMKRs encountered after the first one in an MKB. The CMKR includes a column field. The column field indicates the associated column value for the Device Key to be used with this record. The CMKR also contains encrypted key data in each column corresponding to each of the Device Key rows. Before processing the CMKR, the device checks that the device has a Device Key with associated column value $Cd_i == \text{column}$, for some i .

[0032] If the device does not have a Device Key with the associated column value, the device ignores the rest of the CMKR. Otherwise, using the value i from the condition above, the Device Key and $r = Rd_i$, $c = Cd_i$, the device decrypts a Media Key value from the encrypted key data for row $r = Rd_i$. The resulting Media Key value becomes the current Media Key value.

[0033] A properly formatted MKB may have zero or more conditionally calculated Media Key records (C-CMKR). The C-CMKR contains encrypted conditional data. In the columns, the C-CMKR contains doubly encrypted key data. If decrypted successfully, as described below, the encrypted conditional data contains the hexadecimal value DEADBEEF and the associated column value for the Device Key to be used with this C-CMKR. Using its current Media Key value, the device decrypts conditional data from the encrypted conditional data.

[0034] Before continuing to process the Record, the device checks that the following conditions are true: the decrypted conditional data contains the hexadecimal value DEADBEEF and the device has a Device Key with a newly associated column value (i) decrypted from the conditional data. If any of these conditions is false, the device ignores the rest of the C-CMKR. Otherwise, using the value i from the condition above, the current Media Key value, and $r = Rd_i$, $c = Cd_i$, the device decrypts the doubly encrypted key data at the associated column in the C-CMKR. The device then decrypts the result of the first decryption

of the doubly encrypted data using the device's i-th Device Key. The resulting Media Key becomes the current Media Key value.

Media Key

[0035] When compliant media is placed within a compliant device, a secret Media Key is generated by the device using its secret keys and the Media Key Block stored on the media itself. The same Media Key is generated regardless of which compliant device is used to access the media.

Encrypted Title and Title Key

[0036] Content stored on the media is encrypted/decrypted by a Content Key derived from a one-way function of a secret Title Key and the copy control information (CCI) associated with the content. Encrypted content is hereinafter referred to as "encrypted title". Under the CPRM content protection scheme, the Title Key is encrypted and stored on the media using a key derived from a one-way function of the Media Key and Media ID. The Title Key can subsequently be used to decrypt the content.

Exemplary Embodiment

[0037] In one exemplary embodiment, many concepts related to CPRM, as discussed above, are utilized. In one exemplary embodiment, the invention may be used by an on-line service selling digital content, such as music titles, to its customers. In this embodiment, a Media I.D. corresponding to the original storage medium on which the content is stored is not used (possibly because such ID is not present for the given type of storage media). Instead, a Customer I.D. is obtained that corresponds to a customer purchasing digital content. In the case of music, digital content comprises a music title (hereinafter "title"), for instance.

[0038] Typically, the online service holds music titles (i.e., Content) in encrypted form (Encrypted Title). In an exemplary embodiment, each title is

associated with a secret Title Key with which the title is encrypted, and the Title Key is subsequently encrypted using the Customer I.D. (to be discussed). In alternative embodiments, however, the title may be encrypted using the Customer I.D. rather than the Title Key.

[0039] The online service also holds a Media Key Block (MKB) (rather than the MKB being placed on a medium by a media manufacturer), which is associated with a secret Media Key that is used by an exemplary embodiment to encrypt the Title Key. Both the Title Key and Media Key are subsequently used by a device to decrypt the Encrypted Title. (Where content is bound to a Media I.D., instead of a Customer I.D., the Media I.D. is used with the Media Key to encrypt the Title Key.) In alternative embodiments, the secret Media Key may be used to encrypt the title, and subsequently to decrypt the Encrypted Title.

Binding Content To Customers

[0040] As shown in FIG. 1, when a Customer selects a music title for purchase, certain Customer Information 100 is entered and/or generated, including the Customer I.D. 114, and other information such as the Customer's name, and credit card information. In FIG. 1, the left side of the Network Connection 166 represents the Service, and the right side of the Network Connection 166 represents the Customer.

[0041] The Customer I.D. 114 need not be secret, and may be anything uniquely associated with the Customer. For instance, it could be a full name, login name, or credit card number. Alternatively, it could be a cryptographic hash of one or more of these, or other, values. As another alternative, the Customer I.D. 114 can simply be a unique number assigned to each individual Customer, using a predetermined function by the on-line service. The Customer I.D. may be provided by the Customer, or automatically generated, for instance.

[0042] In an exemplary embodiment in which the title 172 is encrypted 168

using the Title Key 108, the Title Key 108 associated with the selected title is encrypted 110 using a combination 106 (such as a cryptographic one-way function) of the secret Media Key 104 provided by the Service, and the Customer I.D. 114 corresponding to the Customer. In alternative embodiments (shown in broken lines) in which the title 172 is encrypted 170 using the Customer I.D. 114, the selected title is encrypted 170 using a combination 106 (such as a cryptographic one-way function) of the secret Media Key 104 provided by the Service, and the Customer I.D. 114 corresponding to the Customer.

[0043] The MKB 102, Encrypted Title 112, and Encrypted Title Key 116 are also transferred to the Customer, where it can be stored onto a storage medium 160, such as a hard drive or a CD-R disc, which can then be played by the Customer on a device 162.

[0044] FIG. 2 illustrates a high-level method of binding content to a customer I.D. It starts at block 200 and continues to block 202 where a request to transfer content to a customer is received. At block 204, a customer I.D. corresponding to the customer is obtained, and at block 206, the content is bound to the customer I.D. The method ends at block 208.

[0045] FIG. 3 illustrates a detailed method in exemplary embodiments of binding content to a customer I.D. It starts at block 300 and continues to block 302 where a request to transfer content to a customer is received. At block 304, a customer I.D. corresponding to the customer is obtained. At block 306, encrypted content corresponding to the requested content is retrieved, where the encrypted content is encrypted using a title key. At block 308, the content is bound to the customer I.D. by encrypting the title key using the customer I.D. The method ends at block 310.

Accessing Content Bound To Customer I.D.

[0046] In reference back to FIG. 1, the Customer can then connect the

storage medium 160 to a device 162, such as a fixed-function player device, or a computer running player software, for playback. The device 162 reads the MKB 102 from the storage medium 160, and uses its Device Keys 118 to process 164 the MKB 102 in order to calculate the secret Media Key 104.

[0047] In an exemplary embodiment in which the title 172 is encrypted using the Title Key 108, the device 162 reads the Encrypted Title Key 116 from the storage medium 160, and decrypts 120 it using the same combination 106 of the secret Media Key 104 and the Customer I.D. 114 that was used to encrypt the Title Key 108. The result of the decryption 120 is the Title Key 108.

[0048] In one embodiment, the Customer I.D. 114 is taken from the Customer Information 100, transferred to the Customer over the Network Connection 166, and stored on the medium 160. In this embodiment, the content is readily reproduceable and redistributable since the Customer I.D. that is needed to decrypt the content exists on the medium; however, the existence of the Customer I.D. on the medium along with the content acts as a deterrence to distribute the content since the customer knows that the Customer I.D. can be traced back to the customer.

[0049] In another embodiment, the Customer I.D. 114 may be provided by some other means, such as via user input, or otherwise reading it from a system or device local to the user. In this embodiment, the content cannot be reproduced/redistributed unless the correct Customer I.D. 114 is provided via the means.

[0050] In an exemplary embodiment in which the title 172 is encrypted using the Title Key 108, the device 162 reads the Encrypted Title 112 from the storage medium 160, and decrypts 122 it using the Title Key 108 for the purpose of playback 158. In alternative embodiments in which the title 172 is encrypted using the Customer I.D. 114, the device 162 reads the Encrypted Title 112 from the storage medium 160, and decrypts 174 it using the combination of the

Customer I.D. 114 and the Media Key 104. The decrypted title is then available for playback 158.

[0051] FIG. 4 illustrates a high-level method of accessing content that is bound to a customer I.D. The method starts at block 400. At block 402, a customer I.D. is obtained from a customer attempting to access the content. At block 404, the customer I.D. is used to access the content. The method ends at block 406.

[0052] FIG. 5 illustrates a detailed method in exemplary embodiments of accessing content that is bound to a customer I.D. The method starts at block 500. At block 502, the encrypted title key is obtained (i.e., from the medium onto which it is stored from the on-line service), and at block 504, a customer I.D. is obtained from a customer attempting to access the content. At block 506, the encrypted title key is decrypted using the customer I.D, resulting in a title key, and at block 508, the title key is used to decrypt the encrypted content. The method ends at block 510.

Conclusion

[0053] Thus, embodiments of the invention provide an additional or an alternative means for discouraging unauthorized redistribution of protected content by cryptographically binding the content to individual authorized recipients. Since a Customer's identification is bound to a title purchased by the Customer, Customers are further deterred from unauthorized distribution since the title is bound to the Customer and can be traced back to the Customer.

[0054] In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

[0055] While several exemplary embodiments have been described, it should be understood by one of ordinary skill in the art that concepts of this invention are not limited to embodiments discussed herein. For example, concepts of the invention are not limited to the CPRM content protection scheme. As another example, while exemplary embodiments illustrate music titles as content, content is not so limited, and may include other information that is accessed, such as video data and software programs.